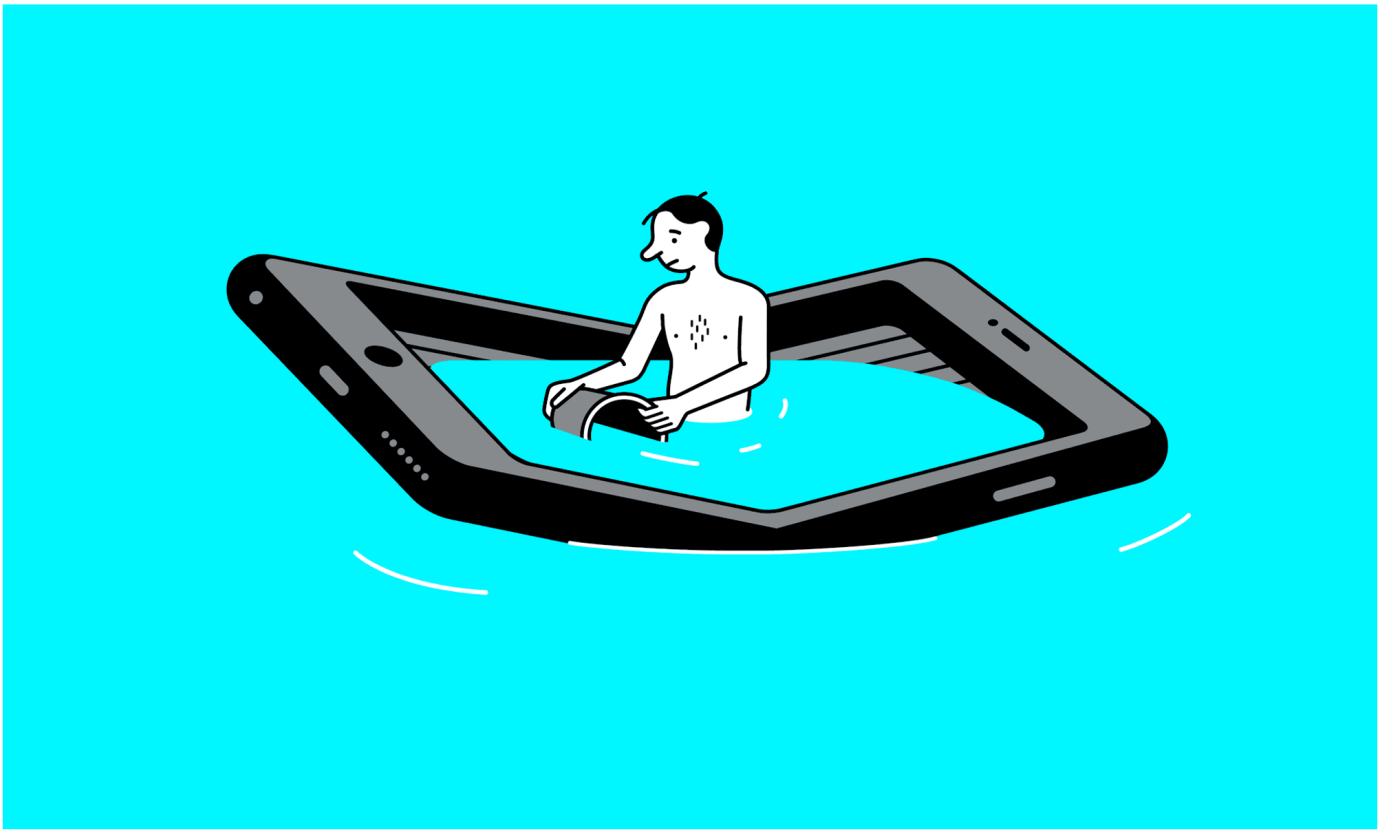

Die DSGVO ist da – und jetzt?

Ihr Postfach quillt momentan über. Für einmal nicht mit Spam, sondern mit aktualisierten Datenschutzbestimmungen. Heute tritt die neue Datenschutzverordnung der EU in Kraft. Wir erklären Ihnen, was Sie als EU-Bürger oder Schweizerin davon haben.

Von Simon Schlauri, Adelina Gashi, Isabelle Schwab (Text) und Till Lauer (Illustration), 25.05.2018

Unverständliche Datenschutzerklärungen, unsichtbares Ausspähen unserer Surfgewohnheiten, versteckte Funktionen, die man auf eigene Initiative ausschalten muss – damit ist ab heute Schluss. Zumindest in den Nachbarländern der Schweiz. Ab heute haben Bürgerinnen und Bürger der EU mehr Möglichkeiten, über ihre Daten zu bestimmen. Unternehmen hingegen sind zu einer umfassenden Transparenz und strengem Datenschutz verpflichtet. Wir erklären die neuen Rechte und Pflichten genauer und zeigen auf, was dies für die Schweiz bedeutet.

Was ändert sich für die EU-Bürger?

Grundsätzlich gilt: Das Verarbeiten von personenbezogenen Daten ist durch die Datenschutzgrundverordnung (DSGVO) verboten. Es gibt nur ei-

nige Fälle, in denen persönliche Daten von Unternehmen verarbeitet werden dürfen. Die drei wichtigsten Rechtfertigungsgründe sind: Datenverarbeitung zur Erfüllung eines Vertrages, mit Einwilligung der betroffenen Person oder bei berechtigtem Interesse.

Welcher Schutz gilt für welche Art Daten?

Sachdaten

Kein Schutz

Personenbezogene Daten

Einfache personenbezogene Daten
IP-Adresse, Name, Alter, Adresse
Einfacher Schutz

Besondere Kategorien personenbezogener Daten
ethnische Herkunft, politische Auffassungen, Gewerkschaftszugehörigkeit, religiöse Überzeugungen, Daten zum Sexualleben, Gesundheitsdaten oder Daten über strafrechtliche Verurteilungen
Erhöhter Schutz

Ein Beispiel: Wenn eine deutsche Kundin ein Sofa bestellt, darf der Lieferant ihre Adresse erfassen und bearbeiten, um seinen Vertrag zu erfüllen und die Ware zu liefern. Er darf jedoch nicht unnötige Informationen verlangen wie beispielsweise ihr Alter. Denn ihr Alter spielt für die Lieferung des Sofas überhaupt keine Rolle. Dieses Koppelungsverbot hat in der Praxis durchaus Auswirkungen: Nicht zweckgebundene Angaben wie das Alter dürfen nur mit Einwilligung verarbeitet werden. Und es ist beispielsweise für einen Web-Shop nicht mehr unter allen Umständen zulässig, von einer Kundin zu verlangen, ein Konto zu eröffnen, denn die Eröffnung eines Kontos ist oft gar nicht nötig für den Kauf.

Die Anforderungen an eine solche Einwilligung sind streng: Sie darf nicht in den allgemeinen Geschäftsbedingungen versteckt sein, sondern muss gesondert ausgewiesen werden. Der Datenschutzerklärung, die die Einwilligung enthält, müssen EU-Bürger dann – etwa durch das Ankreuzen einer Checkbox – explizit zustimmen. Tun sie das, kann das Unternehmen diese Daten auch für andere Zwecke, etwa Marketing, verwenden.

Diese Einwilligung ist jederzeit widerruflich. Auch können EU-Bürgerinnen neu verlangen, dass ihre Daten gelöscht oder berichtigt werden. Ein Löschbegehren gilt dabei nicht nur für das angeschriebene Unternehmen, sondern für alle Parteien, an die die Daten weitergereicht wurden.

Einige Ausnahmen gibt es: Wenn beispielsweise ein berechtigtes Interesse an den Daten besteht, kann keine Löschung verlangt werden. Das ist etwa der Fall, wenn ein Unternehmen rechtliche Ansprüche gegen einen Kunden machen will.

Wichtig ist, dass europäische Betroffene über all diese Vorgänge ins Bild gesetzt werden: Die Rede ist vom Transparenzgrundsatz, der in der neuen DSGVO erheblich ausgeweitet wurde. Personenbezogene Daten müssen gemäss diesem in einer nachvollziehbaren Weise verarbeitet werden. Ein deutscher Kunde hat das Recht auf eine detaillierte Auskunft darüber, ob und welche auf ihn bezogenen Daten verarbeitet werden. Wenn Sie sich beispielsweise fragen, warum die Deutsche Telekom genau mit Ihnen keinen Abonnementsvertrag abschliessen will, muss sie Ihnen Auskunft geben, welche Informationen über Sie zu diesem Schluss geführt haben und woher sie diese Information hat.

Die neue DSGVO sieht ausserdem auch ein neues Recht auf Datenübertragbarkeit vor. Heute schon bietet Facebook in seinen Datenschutzeinstellungen die Möglichkeit, alle gespeicherten Daten auf einmal herunterzuladen. Offen ist, ob die Anbieter sich für die Übertragbarkeit auf einen technischen Standard einigen können.

Die Idee dahinter: Wenn EU-Internetnutzer verlangen können, dass ihre Daten gestützt auf dieses Recht auf andere Plattformen übertragen werden, sind sie eher geneigt, neue Anbieter auszuprobieren und von den grossen Monopolen wie den Gafa (Google, Amazon, Facebook, Apple) dorthin zu wechseln. Manche Start-ups erhoffen sich von diesem Recht auch neue Geschäftsmöglichkeiten.

Hinzu kommt das Recht, bei einer zuständigen Datenschutzbehörde Beschwerde einzulegen. Das war zwar eigentlich schon bisher so; jedoch wird die Drohung angesichts der höheren Bussen säumigen Unternehmen wohl Beine machen.

Auch Schweizerinnen und Schweizer profitieren von diesen neuen Rechten. So sind sie ab heute befugt, eine Auskunft über ihre persönlichen Daten beim Streaming-Dienst Spotify zu verlangen. Weil das Unternehmen seinen Sitz in Stockholm und damit in der EU hat.

Was müssen EU-Unternehmen tun?

Die DSGVO sieht Unternehmen in der Bringschuld: Sie müssen dokumentieren, ob und wie sie die DSGVO umsetzen. Datensicherheitsverletzungen – Leaks – müssen zwingend den Behörden und Betroffenen gemeldet werden. Die neue Rechenschaftspflicht verlangt, dass Unternehmen nachweisen können, dass ihre gesammelten Daten legal bearbeitet werden.

Ausserdem sind die Datenschutz-Einstellungen so datenschutzfreundlich wie möglich voreinzustellen. Wenn Facebook eine französische Nutzerin also fragt, ob sie die neue Gesichtserkennung deaktivieren möchte, dürfte dies eine Verletzung dieses Grundsatzes sein. Denn eigentlich müsste die Gesichtserkennung in Frankreich standardmässig abgeschaltet sein.

Viele kleine und mittlere Betriebe sind durch die umfangreichen Neuerungen überfordert. Deshalb ist Pragmatismus gefragt. Zunächst gilt es, sich den dringlichsten Aufgaben zu widmen. Das heisst, dass man jene Dokumente, die für alle öffentlich verfügbar sind – zum Beispiel im Internet –, an das neue Recht anpasst. Eine Firma, deren online verfügbare Datenschutzerklärung offensichtlich nicht den neuen Standards entspricht, ist ein leichtes Opfer für Behörden und unzufriedene Nutzer.

Das schafft Zeit, sich in einem nächsten Schritt den ganzen anderen mühseligen, aber nötigen Massnahmen zu widmen. So müssen sich Unternehmen nun bewusst die Frage stellen, welche Daten wo und wie verarbeitet werden. Die DSGVO verlangt nämlich nun, dass Firmen mit mehr als 250 Mitarbeitenden darüber eine Liste führen, die sie dann bei Bedarf den Behörden zur Kontrolle vorlegen können.

Was passiert, wenn die Unternehmen die DSGVO-Anforderungen ignorieren?

Unternehmen, die die Vorgaben des neuen Rechts nicht korrekt umsetzen, gehen grosse Risiken ein. Die DSGVO sieht Bussgelder von bis zu 20 Millionen Euro vor oder, im Fall eines Unternehmens, bis zu vier Prozent

des weltweiten Jahresumsatzes, je nachdem, welcher der Beträge höher ist. Gerade die Gafa-Internetriesen riskieren also Milliardenbussen. Auch Privatpersonen und Behörden können bei rechtswidrigen Handlungen gebüsst werden, mit ebenfalls bis zu 20 Millionen Euro.

Das EU-Recht definiert ausserdem neue zivilrechtliche Ansprüche auf Schadenersatz und Genugtuung. Bei Datenschutzverletzungen können neben den Bussen darum auch erhebliche Genugtuungszahlungen fällig werden. Auf Internetriesen wie Facebook oder Google, bei denen die Verarbeitung die Essenz des Geschäftsmodells ausmacht, kommen also möglicherweise bald Milliardenforderungen zu, wenn sie sich nicht anpassen.

Der Datenschutz muss ab heute von allen Unternehmen priorisiert werden. Ein unzufriedener Kunde aus Holland, dessen Datenschutz-Auskunftsersuchen vom unvorbereiteten Kundendienst vergessen wird, kann mit einer Anzeige bei einer Datenschutzbehörde ein internes Debakel auslösen.

Dasselbe gilt für die IT-Abteilung: Im Fall von Datendiebstahl ist in jedem Fall die Juristin einzuschalten, und es ist zu prüfen, ob eine Meldung an die Behörden oder auch die betroffenen Kunden zu machen ist. Auch bei Software-Änderungen oder Änderungen an Prozessen müssen die Datenschutzgrundsätze stets mitgedacht werden.

Die Nervosität ist gross. Viele der in Europa tätigen kleinen und mittleren Unternehmen sind mit der Umsetzung aller Pflichten überfordert, was momentan für einige Unruhe und Besorgnis sorgt.

Die DSGVO fordert jedoch auch die Datenschützer selbst heraus. So wie sich die Unternehmen mit der Umsetzung schwertun, sind nämlich auch die Behörden nicht in der Lage, alle Firmen gleichzeitig zu prüfen. Denn sie haben zwar mehr Pflichten, aber nicht unbedingt mehr Ressourcen für die Aufwandbewältigung. Dadurch geraten zuerst wohl die «grossen Fische» wie die Gafa in den Fokus.

Müssen Schweizer Unternehmen die DSGVO umsetzen?

Unternehmen mit Sitz in der Schweiz können sich nicht zurücklehnen. Nach dem neuen «Marktortprinzip» des europäischen Rechts gilt die DSGVO nämlich auch für Unternehmen ausserhalb der EU und des EWR. Die meisten Schweizer Unternehmen – die Rede ist von siebzig Prozent – müssen sich also sowieso dem europäischen Datenschutzniveau anpassen.

Die Schweiz wird von den EU-Mitgliedstaaten als Drittstaat betrachtet. Derzeit profitiert sie von einem Angemessenheitsbeschluss der Europäischen Kommission. Dieser bescheinigt der Schweiz ein ausreichendes Datenschutzniveau, was den Austausch von Personendaten zwischen der Schweiz und der EU deutlich vereinfacht.

Der Bundesrat geht dabei davon aus, dass sein aktueller Entwurf für ein neues Datenschutzgesetz ausreichend ist, um den Beschluss weiterhin zu gewährleisten. Dies kann sich jedoch angesichts der neuen, höheren Anforderungen der DSGVO wiederum ändern.

Was sind die wichtigsten Unterschiede zwischen der europäischen DSGVO und dem Schweizer DSG?

Ein wichtiges Ziel der aktuellen Überarbeitung des schweizerischen Datenschutzgesetzes (DSG) liegt darin, den schweizerischen Datenschutz EU-kompatibel zu machen. Das Schweizer Datenschutzgesetz ist bereits einige Jahrzehnte alt. Doch das Parlament lässt sich Zeit damit. Die Revision wird erst 2019 so weit sein.

Der Entwurf des neuen Schweizer DSG bleibt in vielen Punkten hinter dem EU-Recht zurück. Einerseits werden die drohenden Bussen in der Schweiz sehr viel tiefer angesetzt als in der EU (nämlich auf maximal 250'000 Schweizer Franken). Andererseits bleiben wesentliche Verletzungen datenschutzrechtlicher Pflichten straflos. So kommt etwa ein Schweizer Unternehmen ungeschoren davon, das ein Datenleck den Behörden pflichtwidrig nicht meldet. Das Datenleck der Swisscom im Herbst 2017 (das jedoch erst anfangs Jahr publik wurde) mit dem Verlust von 800'000 Kundendaten bliebe auch nach dem neuen Schweizer Recht folgenlos für den Telecom-Anbieter.

Schweizerinnen und Schweizer riskieren also beispielsweise bei möglichen Identitätsdiebstählen, dass die verantwortlichen Firmen das Problem lieber unter den Tisch kehren und Stillschweigen darüber bewahren. Dies im Gegensatz zu den Kunden von europäischen Unternehmen, die angesichts der dort drohenden erheblichen Bussen über solche Lecks proaktiv informieren werden.

Verletzungen der meisten allgemeinen Datenschutzgrundsätze bleiben damit zahnlos und werden nicht gebüsst, obwohl sie im bundesrätlichen Entwurf vorgesehen sind. Ein Beispiel: Bei verschiedenen Varianten von Datenschutz-Einstellungen muss die jeweils datenschutzfreundlichste voreingestellt sein. Das heisst, bei Schweizer Nutzerinnen könnte Google beispielsweise die Standortübermittlung des Handys an Google standardmässig eingeschaltet lassen dürfen. Ohne dass eine Busse droht.

Das ist aber noch nicht alles. Nach Schweizer Recht besteht weiterhin keine ausdrückliche Rechenschaftspflicht. Unternehmen, die in der Schweiz tätig sind, müssen also nicht dokumentieren, ob sie den Datenschutz einhalten.

Unklar ist derzeit, ob der Bundesrat das in der EU geltende Koppelungsverbot für die Schweiz übernehmen will. Es könnte demnach sein, dass Unternehmen weiterhin ihre Angebote an die Bedingung knüpfen dürfen, dass Sie als Kundin oder Kunde unnötige Daten bei der Anmeldung online angeben müssen (wie beispielsweise Ihr Alter). Die Einwilligung für die Nutzung der Daten wäre damit nicht mehr «freiwillig» im Sinne des europäischen Rechts.

Auch die Informationspflichten sind nach dem Entwurf des DSG deutlich lascher gefasst als in der DSGVO. Schweizer Unternehmen müssen Kundinnen nicht erklären, aus welchen Gründen ihre Daten verarbeitet werden. Sie müssen sie zudem nicht ausdrücklich und verständlich über ihre Rechte in der Datenschutzerklärung informieren.

Ein eigentliches «Recht auf Vergessenwerden», wie es in der EU ausgestaltet ist, mit einer Weitergabe der Löschpflicht an weitere Datenempfänger, ist in der Schweiz ebenfalls nicht geplant. Nur die verantwortlichen Unternehmen selbst müssen die Daten auf Anweisung der betroffenen Person löschen.

Die Unterschiede in der Übersicht

Europäische DSGVO und Schweizer DSG. Was gilt wo?

	EU	CH
Hohe Bussen	✓	×
Rechenschaftspflicht	✓	×
Meldepflicht	✓	×
Datenübertragbarkeit	✓	×
Koppelungsverbot	✓	?
Informationspflicht	✓	(✓)
Recht auf Vergessen	✓	(✓)

Die Differenzen zwischen dem bundesrätlichen Entwurf und der DSGVO sind teilweise doch erheblich gross. Es besteht deshalb das Risiko, dass die EU die Gleichwertigkeit des neuen schweizerischen Rechts mit der DSGVO nicht mehr anerkennt. Die enge Verzahnung mit dem europäischen Binnenmarkt führt dazu, dass auf die meisten Schweizer Unternehmen auch das europäische Recht anwendbar sein wird. Somit würde eigentlich kaum ein Schweizer Unternehmen von einem «liberalen» Schweizer Datenschutzrecht profitieren.

Schweizerinnen und Schweizer profitieren derweil von den EU-Unternehmen und von den «EU-kompatiblen» Schweizer Unternehmen. Schweizer Unternehmen dürften künftig kaum den Aufwand betreiben, für Kunden aus der Schweiz und der EU verschiedene Datenschutzstandards anzuwenden. Sie werden stattdessen einfach den strengeren EU-Regeln folgen.

Für die Schweizer Wirtschaft wäre es jedoch fatal, wenn die EU die Schweizer Bestimmungen nicht als gleichwertig anerkennt. Die Zusammenarbeit von europäischen mit Schweizer Unternehmen würde so administrativ komplizierter. Und die bisher als zuverlässig geltende Schweizer IT-Branche erhielte das Label «Datenschutz ungenügend».

Debatte: DSGVO: Alles unklar?

Diskutieren Sie heute von 9.30 bis 17 Uhr mit unserer Expertinnenrunde: Was geht Sie die DSGVO eigentlich an? Soll die Schweiz mit der EU nachziehen oder eine eigene Lösung anbieten? Muss ich ab sofort auf bestimmte Fragen von Unternehmen besonders aufpassen? Hier gehts zur Debatte.

Zum Autor

Simon Schlauri ist Republik-Verleger, IT-Anwalt bei Ronzani Schlauri Anwälte und seit Mai 2018 Zürcher Kantonsrat.